Akamai

LIVRE BLANC

Plan d'action pour les 10 principaux risques liés à la sécurité des API identifiés par l'OWASP

Comment Akamai peut vous aider à résoudre les vulnérabilités et les menaces courantes liées aux API

Liste des 10 principaux risques pour la sécurité des API de l'OWASP		Les produits d'Akamai peuvent-ils vous aider ?
API1 : 2023	Autorisation brisée au niveau de l'objet	☑
API2 : 2023	Violation d'authentification	☑
API3 : 2023	Autorisation brisée au niveau de la propriété de l'objet	☑
API4 : 2023	Consommation de ressources illimitée	☑
API5 : 2023	Autorisation brisée au niveau de la fonction	☑
API6 : 2023	Accès illimité aux flux d'activité sensibles	☑
API7 : 2023	Falsification de requête côté serveur	☑
API8 : 2023	Mauvaise configuration de sécurité	☑
API9 : 2023	Mauvaise gestion des stocks	☑
API10 : 2023	Consommation d'API non sécurisée	☑

Les API sont au cœur des produits digitaux, des services et des environnements cloud d'une entreprise. Elles sont également indispensables pour créer et connecter des applications, les entreprises adoptant de plus en plus une architecture basée sur les microservices pour développer leurs applications. Cependant, l'accès constant de ces API aux données et aux systèmes critiques en fait à la fois une source de revenus et un risque opérationnel.

Les API exposées ou mal configurées sont courantes, faciles à compromettre et souvent non protégées. Une seule API compromise peut entraîner le vol de millions d'enregistrements.

Alors que 78 % des entreprises déclarent avoir subi des incidents de sécurité liés aux API en l'espace d'un an, il est clair que la protection des API doit être une priorité. Cependant, la surface d'attaque des API est rapidement devenue une cible de choix, ce dont de nombreuses entreprises n'ont pas encore pris conscience :

Risques liés aux API

Méthodes d'attaque des API

Fonctionnalités et contrôles de sécurité des API

Que comprend la surface d'attaque des API ? En résumé, cette surface est bien plus étendue que ne le pensent de nombreuses organisations. La perception traditionnelle des API (telles que les API d'interface machine ou les API tierces) peut et doit être développée afin d'inclure les services d'applications mobiles et Web dans l'architecture basée sur les microservices. En d'autres termes, une requête Web au sein de l'architecture est une API qui fait partie d'une série d'appels destinés à différents microservices.

78 %

des organisations déclarent avoir subi des incidents de sécurité liés aux API en l'espace d'un an. Il est clair que la protection des API doit être une priorité.

Le 5 juin 2023, le très respecté OWASP (Open Worldwide Application Security Project) a publié la première mise à jour majeure de sa liste des 10 principaux risques pour la sécurité des API, publiée en 2019. La nouvelle liste indique comment chacun de ces appels d'API peut potentiellement créer des failles de sécurité et entraîner des risques pour la vie privée :

Mauvaise validation des données

Erreurs de configuration

Défauts de mise en œuvre

Intégration insuffisante entre les composants de sécurité

Lisez la suite pour découvrir les principaux risques identifiés par l'OWASP et comment les solutions de sécurité des API d'Akamai peuvent vous aider à les atténuer.

Malheureusement, même les organisations qui prétendent avoir effectué un inventaire complet de leurs API présentent de sérieuses lacunes :

Seules **4 entreprises sur 10** savent laquelle de leurs API renvoie des données sensibles lors d'un appel.

API1 : 2023 — Autorisation brisée au niveau de l'objet

Les vulnérabilités liées à une autorisation brisée au niveau de l'objet (Broken Object Level Authorization, BOLA) peuvent être présentes lorsqu'une autorisation d'accès à des ID d'objets spécifiques n'est pas correctement validée par un client. Cette vulnérabilité peut permettre aux pirates d'accéder directement aux ressources, en contournant le workflow d'application prévu et en obtenant un accès non autorisé à des données sensibles. Les entreprises peuvent réduire ce risque en évitant de se fier uniquement aux ID d'objet que les clients transmettent dans leurs demandes et en utilisant des ID d'objet aléatoires et impossibles à deviner afin de garantir une validation efficace pour chaque objet. Le cas échéant, le masquage du véritable ID d'objet peut apporter une couche de sécurité supplémentaire.

Comment Akamai peut vous aider

Les systèmes de surveillance vigilants d'Akamai suivent les menaces et génèrent des alertes en cas de tentative d'exploitation de vulnérabilités BOLA, ce qui garantit une attention et une action immédiates.

Akamai atténue le risque :

- en identifiant les tentatives d'exploitation de vulnérabilités BOLA ;
- en classifiant les points de terminaison d'API susceptibles d'être exploités par une vulnérabilité BOLA en fonction des entrées reçues (ex. : paramètres énumérables), ainsi que des relations entre les objets API et les propriétés ;
- en déclenchant des alertes en cas de tentative d'exploitation ou d'exploitation avérée de vulnérabilités BOLA.

API2 : 2023 — Violation d'authentification

La violation d'authentification (Broken Authentication, BA) désigne d'importantes vulnérabilités dans le processus d'authentification, exposant le système à des pirates qui peuvent exploiter ces faiblesses pour compromettre la protection des objets API. En général, les pirates qui exploitent des vulnérabilités liées à une violation d'authentification manipulent des failles dans le système (par exemple, des mots de passe faibles ou la réplication de session). Pour se protéger contre les failles de violation d'authentification, les entreprises peuvent établir des mécanismes d'authentification et de gestion des secrets robustes, dont des stratégies de mots de passe forts, une rotation de clés, des signatures de jeton fortes et des clés de chiffrement. L'application de ces règles strictes dans l'ensemble de l'entreprise peut réduire considérablement les risques.

Comment Akamai peut vous aider

Akamai renforce la sécurité des API en identifiant et en corrigeant les points d'authentification faibles, en déjouant les attaques automatisées et en déclenchant des alertes en amont en cas de tentative d'exploitation.

Akamai atténue ce risque :

- en identifiant les points de terminaison d'API qui ne nécessitent aucune authentification ou qui ne respectent pas les meilleures pratiques en matière d'authentification, telles que les signatures de jeton et les clés de chiffrement faibles ou l'acceptation de jetons d'authentification périmés ;
- en assurant une protection contre les attaques automatisées par dictionnaire ou par credential stuffing, à l'aide de nos fonctionnalités de gestion des bots ;
- en gérant l'autorisation des jetons Web JSON à l'aide de signatures de jetons fortes via les fonctionnalités de notre solution de passerelle d'API ;
- en déclenchant des alertes en cas de tentative d'exploitation de vulnérabilités BA.

API3 : 2023 — Autorisation brisée au niveau de la propriété de l'objet

L'autorisation brisée au niveau de la propriété de l'objet (Broken Object Property Level Authorization, BOPLA) est une faille de sécurité qui permet à un point de terminaison d'API d'exposer inutilement davantage de propriétés de données que nécessaire pour sa fonction, négligeant ainsi le principe du moindre privilège.

Cette faille peut, par inadvertance, mettre une grande quantité de données à disposition des pirates, qu'ils peuvent ensuite utiliser pour détecter d'autres vulnérabilités ou pour extraire des données sensibles. Ainsi, des propriétés exclusivement associées à un accès de niveau administrateur peuvent être manipulées par des utilisateurs non autorisés, au point de compromettre encore davantage l'intégrité du système. Pour garantir la sécurité et empêcher les pirates d'obtenir ou de manipuler des informations en quantité excessive, il est essentiel de fournir des niveaux d'accès et une exposition aux données appropriés, de manière à empêcher les pirates potentiels de tirer profit de ces négligences.

Comment Akamai peut vous aider

Les tactiques complètes d'Akamai permettent aux entreprises d'atténuer les risques liés aux vulnérabilités BOPLA, en identifiant et en cataloguant les points de terminaison d'API et leurs propriétés associées.

Akamai atténue ce risque :

- en identifiant et en étiquetant tous les points de terminaison et les propriétés d'API qu'ils exposent, notamment les informations d'identification personnelles (PII) ;
- en identifiant les points de terminaison, les objets et les propriétés d'API non documentés ou fantômes, ainsi que les propriétés anormales ;
- en appliquant des règles de sécurité sur des paramètres et des propriétés acceptables et définis afin de garantir le nettoyage des données ;
- en appliquant des règles de sécurité entièrement basées sur la spécification OpenAPI/Swagger, et en autorisant uniquement des points de terminaison et des méthodes d'API bien définis à accéder aux objets et propriétés d'API ;
- en déclenchant des alertes en cas de tentative d'exploitation de vulnérabilités BOPLA.

API4 : 2023 — Consommation illimitée des ressources

La consommation illimitée des ressources (parfois qualifiée d'épuisement des ressources d'API) désigne un type de vulnérabilité dans lequel les API ne limitent pas le nombre de requêtes ou le volume de données qu'elles traitent dans un délai donné. Cette négligence est du pain béni pour les pirates qui cherchent à lancer des attaques par déni de service (DoS), car elle peut empêcher les utilisateurs légitimes d'accéder au système. L'exploitation de ce type de faille peut entraîner de lourdes conséquences économiques : indisponibilité du service, clients mécontents, pertes de revenus potentielles, dont l'ampleur dépend de la durée et de l'étendue de la panne. Il est essentiel de mettre en place des mesures qui limitent le taux de requêtes API et le volume des retours de données afin d'éviter la perte de service.

Comment Akamai peut vous aider

Akamai protège vos API contre les menaces liées à la consommation illimitée de ressources :

- en identifiant les points de terminaison à risque et en générant des alertes en temps réel sur les tentatives d'attaques volumétriques ;
- en détectant les erreurs excessives, les tentatives de connexion ou les comportements atypiques indiquant un risque.

Akamai atténue ce risque :

- en identifiant les points de terminaison d'API pour lesquels aucune limite de débit n'a été fixée ou qui subissent de grandes attaques par dictionnaire volumétrique ou par credential stuffing ;
- en lançant des flux de travail pour ralentir ou bloquer les attaques volumétriques ;
- en générant des alertes en cas de tentative d'attaque volumétrique.

API5 : 2023 — Autorisation brisée au niveau de la fonction

Une autorisation brisée au niveau de la fonction (Broken Function Level Authorization, BFLA) peut se produire à la suite d'une mise en œuvre incorrecte des modèles de contrôle d'accès pour les points de terminaison d'API. Des méthodes de contrôle d'accès incorrectes ou obsolètes risquent de ne pas limiter les accès non autorisés comme il se doit, au point de laisser les pirates accéder à des informations sensibles, voire à l'ensemble du système. Pour atténuer ce risque, les entreprises peuvent adopter le principe du moindre privilège, en veillant à ce que toutes les fonctions (en particulier les fonctions administratives) ne soient accessibles qu'aux utilisateurs disposant des autorisations appropriées.

Comment Akamai peut vous aider

En suivant les chronologies comportementales, en appliquant des règles de sécurité aux fonctions sensibles, en gérant la rotation et la révocation des clés et en alertant rapidement de toute tentative suspecte, Akamai peut renforcer la stratégie de prévention et de réponse des entreprises face aux vulnérabilités BFLA.

Akamai atténue ce risque :

- en consignant les ID utilisateur, les clés d'API, les jetons d'accès, les identifiants de session, etc. pour identifier des chronologies comportementales concernant l'accès aux points de terminaison d'API ;
- en gérant la rotation des clés ou la révocation des clés exposées à l'aide de la passerelle d'API d'Akamai ;
- en générant des alertes en cas de tentative suspecte d'accès aux fonctions administratives.

API6 : 2023 — Accès illimité aux flux d'activité sensibles

L'accès illimité aux flux d'activité sensibles est un risque qui survient lorsqu'une API expose des opérations critiques, telles que la logique métier, sans contrôle d'accès suffisant. Cela peut conduire à un accès non autorisé et à une exploitation de vulnérabilité, infligeant des dommages importants à une organisation. L'exploitation implique généralement de comprendre le business model étayé par l'API, d'identifier les flux métier sensibles et d'exploiter les angles morts de ces flux. Entre autres conséquences, cela peut empêcher des utilisateurs légitimes d'acheter un produit.

Comment Akamai peut vous aider

Sécurisez votre entreprise avec les solutions complètes de protection des API d'Akamai, conçues pour identifier les points de terminaison sensibles, déclencher des alertes d'exploitation en temps réel et fournir des conseils d'experts afin de protéger vos données et opérations critiques.

Akamai atténue ce risque :

- en identifiant les points de terminaison d'API sensibles, tels que les flux de paiement ou les points de terminaison qui gèrent les informations personnelles identifiables ;
- en générant des alertes sur différents types d'exploitations potentielles, allant de l'exfiltration à la manipulation de données, en passant par les tentatives suspectes sur ces points de terminaison d'API sensibles.

API7 : 2023 — Falsification de requête côté serveur

La falsification de requête côté serveur (Server Side Request Forgery, SSRF) permet à un pirate d'inciter l'application côté serveur à adresser des requêtes HTTPS à un domaine arbitraire de son choix. Dans le cadre d'une attaque SSRF type, le pirate trompe le serveur afin qu'il lance une requête sur les ressources internes, de manière à contourner les pare-feux et à accéder aux services internes, ce qui peut conduire à une exposition des données ou à l'exécution de code à distance. Pour atténuer ce risque, il est crucial de valider, filtrer ou nettoyer les saisies utilisateur et de limiter les connexions sortantes que votre serveur peut établir, en veillant à ce qu'il communique uniquement avec les services critiques.

Comment Akamai peut vous aider

Akamai renforce votre stratégie de sécurité en détectant les anomalies dans les connexions API fiables, en gérant efficacement les clés et en envoyant des notifications immédiates chaque fois qu'une tentative d'exploitation de vulnérabilité SSRF est détectée.

Akamai atténue ce risque :

- en appliquant une protection par le biais de règles de protection d'applications Web et d'API qui ciblent les attaques SSRF ;
- en gérant la rotation des clés ou la révocation des clés exposées à l'aide des fonctionnalités d'API Gateway.

API8 : 2023 — Mauvaise configuration de sécurité

Une mauvaise configuration de sécurité désigne une configuration incorrecte des contrôles de sécurité, qui peut rendre un système vulnérable aux attaques. Il peut s'agir, par exemple, de configurations par défaut non sécurisées, de configurations ad hoc ou incomplètes, d'un stockage dans le cloud, d'en-têtes HTTP(S) mal configurés ou de messages d'erreur détaillés contenant des informations sensibles. Pour atténuer ces risques, il est essentiel que les organisations veillent à configurer correctement leurs contrôles de sécurité sur tous les aspects de leurs applications et de leurs API. Cela implique des mises à jour régulières, des tests approfondis et une surveillance continue pour identifier et corriger rapidement toute erreur de configuration.

Comment Akamai peut vous aider

Akamai vous aide à obtenir une meilleure visibilité en identifiant les points de terminaison d'API « fantômes », « malveillantes » ou « zombies » et à adopter les meilleures pratiques de sécurité, avec une implémentation HTTPS efficace et des alertes instantanées en cas de mauvaise configuration de sécurité.

Akamai atténue ce risque :

- en identifiant les points de terminaison d'API « fantômes » susceptibles d'exposer des environnements de bas niveau (ex. : environnements de test et de staging) ;
- en identifiant les points de terminaison, les objets et les propriétés d'API, et en leur appliquant les normes et les meilleures pratiques en matière de configuration de sécurité ;
- en appliquant des règles de sécurité fondées sur les meilleures pratiques de sécurité des API, notamment des requêtes et des réponses HTTPS bien formulées, la configuration ou la suppression d'en-têtes HTTP corrects, ou encore le contrôle total du partage de ressources inter-origines (CORS) et les en-têtes de contrôle du cache ;
- en appliquant une implémentation HTTPS appropriée via le protocole SSL/TLS, avec des suites de chiffrement correctes et sécurisées ;
- en générant des alertes en cas de mauvaise configuration ou de non-respect des meilleures pratiques et normes de sécurité des API.

API9 : 2023 — Mauvaise gestion des stocks

La mauvaise gestion des stocks représente un véritable défi pour toute organisation qui gère des API. Les solutions de sécurité des API protègent les API connues. Toutefois, les API inconnues, telles que les API fantômes, peuvent ne pas être corrigées et être vulnérables aux attaques. Cette vulnérabilité peut engendrer des composants obsolètes, des pages ou des API inutilisées et une exposition inutile des informations sensibles. Une gestion des services laissée à l'abandon peut rendre les systèmes vulnérables aux menaces, avec le risque que des pirates accèdent à des données sensibles, voire au serveur à proprement parler, via des API inconnues connectées à la même base de données. Il est essentiel de réaliser des contrôles d'accès et des audits réguliers pour éviter de modifier en permanence les composantes des services d'une entreprise.

Comment Akamai peut vous aider

Akamai supervise en permanence le trafic d'API pour aider à découvrir les points de terminaison d'API cachés et les API présentant des risques potentiels, afin de garantir un stockage sécurisé des données, de réaliser une analyse avancée des menaces et de générer des alertes immédiates en cas d'exploitation potentielle.

Akamai atténue ce risque :

- en surveillant en permanence le trafic d'API exposé circulant dans vos environnements, y compris les points de terminaison d'API nord-sud ciblant les API accessibles au public et les points de terminaison d'API internes est-ouest ;
- en identifiant les points de terminaison d'API « fantômes » susceptibles d'exposer des environnements de bas niveau (ex. : environnements de test et de staging) ou les versions d'API non documentées et/ou obsolètes ;
- en créant un inventaire des API à jour, basé sur la notation des risques et la classification des données ;
- en générant des alertes sur différents types d'exploitations potentielles, allant de l'exfiltration à la manipulation de données, en passant par les tentatives suspectes sur ces points de terminaison d'API sensibles.

API10 : 2023 — Consommation d'API non sécurisée

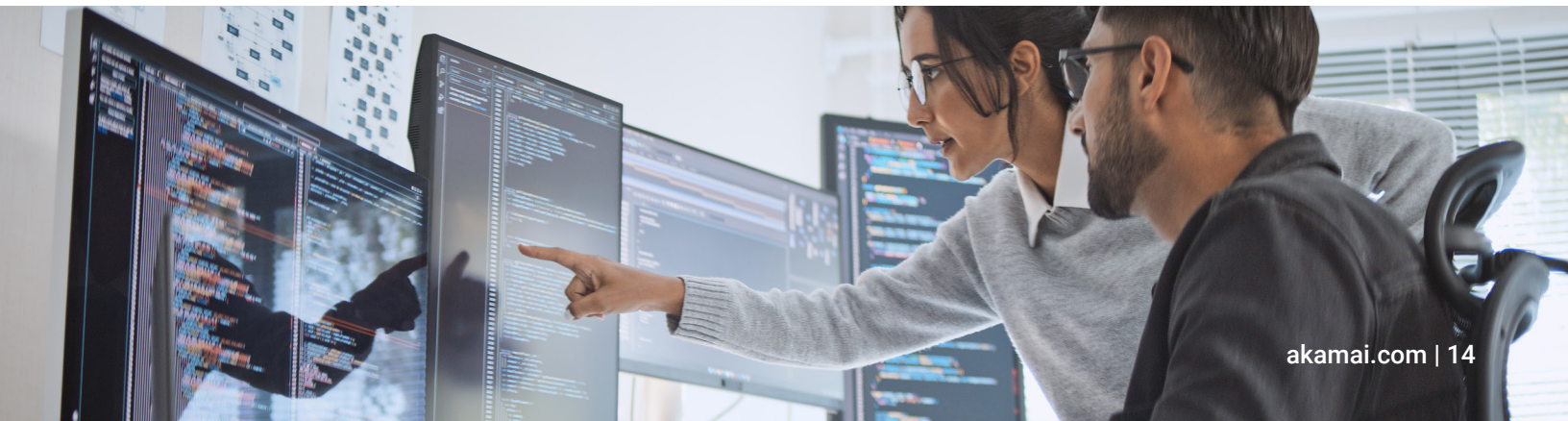
La consommation d'API non sécurisée désigne les risques associés à l'utilisation d'API tierces sans mettre en place de mesures de sécurité appropriées. Les entreprises utilisent de plus en plus d'API tierces pour étendre leurs services et fonctionnalités. De ce fait, elles font souvent confiance à ces API par défaut, ce qui peut entraîner des failles de sécurité importantes. Les entreprises qui omettent d'appliquer certains contrôles appropriés (chiffrement, validation des données, nettoyage, limites de consommation des ressources) peuvent s'exposer à des vulnérabilités importantes. Pour atténuer ces risques, les entreprises peuvent chiffrer toutes les données transmises sur le réseau, valider et nettoyer toutes les entrées de données et fixer des limites raisonnables pour la consommation des ressources.

Comment Akamai peut vous aider

Misez sur les services de surveillance, d'émission d'alertes et de conseil d'Akamai pour protéger en permanence vos systèmes en surveillant et en validant vos services afin d'en garantir la sécurité.

Akamai atténue ce risque :

- en assurant une surveillance continue du trafic d'API exposé circulant dans vos environnements, y compris les API est-ouest et sortantes qui facilitent les intégrations B2B et/ou tierces ;
- en générant des alertes sur différents types d'exploitations potentielles, allant de l'exfiltration à la manipulation de données, en passant par les tentatives suspectes sur ces points de terminaison d'API sensibles ;
- en appliquant une protection par le biais de règles de protection d'applications Web et d'API qui ciblent différentes attaques d'API rassemblées dans des groupes d'attaques.



Risques de sécurité supplémentaires selon l'OWASP

La liste 2023 des 10 principaux risques pour la sécurité des API de l'OWASP est la première mise à jour majeure de la liste de l'organisation à but non lucratif depuis 2019. Il n'est toutefois pas inutile de consulter la liste d'origine, qui aborde d'autres risques de sécurité, tels que les attaques par injection, qui sont toujours d'actualité.

Akamai peut vous aider à atténuer ce risque :

- en identifiant les cas d'injection API (points de terminaison vulnérables et tentatives d'injection) par une mise en correspondance des signatures et une détection des anomalies ;
- en appliquant des règles de sécurité via une inspection JSON et XML des requêtes API et par la recherche de différents types d'attaques par injection (SQLi, XSS, CMDi, RFI et LFI) ;
- en déclenchant des alertes en cas d'exploitation par injection.

L'OWASP a également publié des listes des 10 principaux risques liés à la sécurité, notamment les 10 principaux risques liés à la sécurité des applications Web identifiés par l'OWASP. La gamme de solutions de sécurité d'Akamai peut également contribuer à atténuer ces risques de sécurité.

Nous sommes là pour vous aider !

Les entreprises et leurs fournisseurs de solutions de sécurité doivent travailler en étroite collaboration, en alignant l'ensemble des utilisateurs, des processus et des technologies afin d'établir une défense solide contre les risques de sécurité décrits dans la liste des 10 principaux risques pour la sécurité des API de l'OWASP.

Akamai met à votre disposition des solutions de sécurité de pointe, des experts hautement qualifiés et une plateforme qui rassemble chaque jour des informations sur des millions d'attaques d'applications Web et d'API, des milliards de requêtes de bots et des milliers de milliards de demandes d'API.

Les solutions de sécurité des applications Web et API d'Akamai vous aideront à protéger votre entreprise contre les formes les plus avancées d'attaques d'applications Web, DDoS et basées sur les API. De plus, la solution Managed Security Service d'Akamai assure une gestion de la sécurité, une atténuation des menaces et une surveillance 24 h/24, 7 j/7.

Pour en savoir plus sur les solutions de sécurité d'Akamai, consultez notre site Web. Si vous souhaitez discuter en détail des solutions que nous proposons pour créer la protection la mieux adaptée à votre entreprise, contactez dès maintenant votre représentant commercial Akamai.

Akamai Security protège les applications qui stimulent votre activité à chaque point d'interaction, sans compromettre les performances ou l'expérience client. En tirant parti de l'envergure de notre plateforme mondiale et de la visibilité qu'elle offre sur les menaces, nous travaillons avec vous pour prévenir, détecter et atténuer les menaces, afin de vous permettre de renforcer la confiance en votre marque et de concrétiser votre vision. Pour en savoir plus sur les solutions de Cloud Computing, de sécurité et de diffusion de contenu d'Akamai, rendez-vous sur akamai.com et akamai.com/blog, ou suivez Akamai Technologies sur X (anciennement Twitter) et LinkedIn. Publication : 09/24.